Listing of Claims:

Claim 1: (Previously Presented) An apparatus comprising:

a firewall configured to:

receive data packets over a first network;

classify the received data packets based on the contents of the data packets into packets of a first type which cannot contain a virus and packets of a second type which can contain a virus;

forward the data packets of the first type to a destination without testing by a virus scanning engine; and

forward the data packets of the second type to a virus scanning engine for testing.

Claims 2-3: (Canceled)

Claim 4: (Previously presented) The apparatus of claim 1, wherein the classifying comprises determining that data packets of the first type contain real time data.

Claim 5: (Previously presented) The apparatus of claim 4, wherein the classifying comprises determining that data packets of the first type are part of an audio or video data stream.

Claim 6: (Previously presented) The apparatus of claim 1, wherein the firewall is configured to stop reception of a data stream containing the data packets in response to an alert from the virus scanning engine.

Claims 7-10: (Canceled)

Claim 11: (Previously presented) The apparatus of claim 1, further comprising a buffer configured to store the data packets of the second type while the virus scanning engine is testing the data packets to detect a virus.

Claims 12-31: (Canceled)

Claim 32: (Previously presented) The apparatus of claim 1, wherein the firewall is configured to receive from a packet classification database information defining the first and second types of data packets.

Claim 33: (Previously presented) The apparatus of claim 32, further comprising:

a virus scanning engine configured to receive from a virus detection database programming information controlling the testing of the data packets of the second type by the virus scanning engine.

Claim 34: (Previously presented) The apparatus of claim 1, further comprising:

a virus scanning engine configured to receive from a virus detection database programming information controlling the testing of the data packets of the second type by the virus scanning engine.

Claims 35-39: (Canceled)

Claim 40: (Previously presented) The apparatus of claim 1, further comprising a virus scanning engine configured to alert the destination upon detection of a virus in the data packets.

Claim 41: (Previously presented) The apparatus of claim 1 wherein the destination is a local area network.

Claim 42: (Previously presented) The apparatus of claim 1 wherein the destination is a personal computer.

Claim 43: (Previously presented) The apparatus of claim 1, wherein the destination is a second network.

Claim 44: (Previously presented) The apparatus of claim 1, wherein the first network is a wide area network.

Claim 45: (Previously presented) The apparatus of claim 44, wherein the wide area network is the Internet.

Claim 46: (Previously presented) The apparatus of claim 1, wherein

the destination comprises an Internet service provider configured to connect to a gateway, a modem configured to connect to the Internet service provider, and one of a local area network or personal computer configured to connect to the modem.

Claim 47: (Previously presented) The apparatus of claim 1, further comprising a virus scanning engine configured to decode the data packets during the testing of the data packets.

Claim 48: (Previously presented) The apparatus of claim 47, wherein the virus scanning engine is configured to function as a proxy for a destination processor configured to receive the data packets.

Claim 49: (Previously Presented) A method comprising:

receiving data packets;

classifying the data packets based on the contents of the data packets into packets of a first type which cannot contain a virus and packets of a second type which can contain a virus;

transmitting the received data packets of the first type to a destination without testing by a virus scanning engine; and

transmitting the received data packets of the second type to a virus scanning engine for testing.

Claim 50: (Previously Presented) A computer program stored on a storage medium comprising computer executable instructions for performing a method comprising:

receiving data packets;

classifying the received data packets based on the contents of the data packets into packets of a first type that cannot contain a virus and packets of a second type that can contain a virus;

transmitting the data packets of the first type to a destination without testing by a virus scanning engine; and

transmitting the data packets of the second type to a virus scanning engine for testing.

Claims 51-52: (Canceled)

Claim 53: (Previously presented) A computer program in accordance with claim 50, wherein the classifying comprises determining that data packets of the first type contain real time data.

Claim 54: (Previously presented) A computer program in accordance with claim 50, wherein:

the computer program when executed causes reception of a data stream containing the data packets to be stopped in response to an alert from the virus scanning engine.

Claim 55: (Canceled)

Claim 56: (Previously presented) A computer program in accordance with claim 50, wherein the method further comprises receiving from a packet classification database information defining first and second types of data packets.

Claim 57: (Previously presented) A computer program in accordance with claim 53, wherein the classifying further comprises determining that data packets of the first type are part of an audio or video data stream.

Claim 58: (Previously presented) The method of claim 49, wherein the classifying comprises determining that data packets of the first type contain real time data.

Claim 59: (Previously presented) The method of claim 58, wherein the classifying further comprises determining that data packets of the first type are part of an audio or video data stream.

Claim 60: (Previously presented) The method of claim 49, further comprising receiving information from a packet classification database, said information defining the first and second types of data packets.

Claim 61: (Previously presented) The method of claim 49, wherein the classifying is performed by a firewall.

Claim 62: (Previously Presented) An apparatus, comprising:

a processor; and

memory storing computer executable instructions that, when executed by the processor, cause the apparatus to:

receive data packets;

classify the data packets based on the contents of the data packets into packets of a first type which cannot contain a virus and packets of a second type which can contain a virus;

transmit the data packets of the first type to a destination without testing by a virus scanning engine; and

transmit the data packets of the second type to a virus scanning engine for virus testing.

Claim 63: (Previously presented) The apparatus of claim 62, wherein the classifying comprises determining that data packets of the first type are part of a real-time audio or video data stream.

Claim 64: (Previously presented) The method of claim 49, wherein classifying the data packets based on the contents of the data packets includes determining whether at least one of the data packets includes content for a real-time audio or video data stream.

Claim 65: (Previously Presented) A computer program in accordance with claim 50, wherein the classification is performed by a firewall.